REPORT ON INTERROGATION OF KOMMANDEUR DER NACHR. AUFKL. 1 (KONA 1) AT REVIN, FRANCE, JUNE 1945

A N N E X E 2

(TRAFFIC ANALYSIS)

* * * * *

TICOM
1 July 1945

Copy No. 16
No. of Pages 11

Distribution:

British
1. Director
2. D.D.3.
3. D.D.4.
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R.) (2)
9. Lt.Col. Leathem

U.S.
26-27. OP-20-G (2) (via Lt. Pendergrass)
28. G-2 (via Lt.Col. Hilles)
29-30. S.S.A. (2) (via Major Seaman)
31. Director, S.I.D. ETOUSA (via Lt. Col. Johnson)

TICOM
10. Chairman
11-12. S.A.C. (2)
13. Cdr. Bacon
14. Cdr. Mackenzie
15. Cdr. Tandy
16. Lt.Col. Johnson
17. Lt.Cdr. Manson
18. Major Seaman
19. Lieut. Eachus
20. Lieut. Vance
21. Captain Cowan
22. Lieut. Fehl
23-25. TICOM Files (3)

Additional
32-33. Lt.Col. Pritchard (2)

TRAFFIC ANALYSIS

(Adapted from die Funkbetriebsforschung
by Uffz. Wilhelm Heimann, NAAS/T.)

INTRODUCTION

T.A. comprises the investigation of frequency and callsign usage.

A. The study of frequency usage did not produce results to any appreciable extent which could have been used to re-identify W/T networks after change of frequency. Therefore, apart from periodic tests, the systematic study of frequency changes was abandoned as unproductive.

B. Study of Callsigns.

Its purpose was to establish:

1) Callsign books or systems (Unterlagen) from which callsigns were drawn.

2) The manner of callsign selection.

3) The various groups of callsign users.

The objective was to determine, on the basis of callsigns, the character of a given wireless network; further to identify formations in that network, and, then, to maintain continuity through callsign changes.

Expansion of B. - The Study of Callsigns

B.1 Callsign Systems

There were found to be two different tables of callsigns.

TFR.43: A list of 1200 words, the first three letters of which were used in keying traffic, and
Callsign Books, each with 1100/1200 callsigns, which were compiled of letters and figures in such a manner that (excepting compilers' errors) identical callsigns could not occur.

TFR.43 had 16 pages, 75 callsigns per page, divided into three groups, each of 25 callsigns. Each group had 5 lines, each with 5 callsigns.

(The above is based on captured documents.)

From the numbering of captured documents the approximate scope of this material can be estimated at about 17 to 18 books. Up till now about 12 or 13 books have been in use. Books were not compiled as complete books but approximately 200 pages were first compiled and then split up into books. Each page contains 96 callsigns beginning with 32 different characters, 3 callsigns per character, and 4 callsigns beginning with 2 other characters, 2 callsigns per character. No callsign began with Ä, Z, R, U, Q and Ö. (The 34 characters therefore used as beginners were: A, B, W, G, D, V, I, J, K, L, M, N, O, P, S, T, F, H, C, Ü, CH, Y, X, Ü, Ä, 1, 2, 3, 4, 5, 6, 7, 8, 9. The unused beginners are obviously those likely to be confused with Russian International callsigns, operating signals, etc.)

Since the 34 beginners would have yielded 3 x 34 = 102 callsigns, 2 beginners in rotation were selected to form 2 callsigns each.

The affiliation of the books could thus be recognised by knowing which 2 initial characters on each page were those limited to form 2 callsigns each.

To keep check on the allocation of callsigns to individual pages the compiler used a list in which the 34 initial characters each had 2 sheets, one extending from A to C and the other from Ö to 9. (See Figure 1.) *

The compiler, having derived the callsign, say, AAA, entered it in any position on a page which was then apportioned to one of the 17 or 18 books. The designation of its location, in terms of page and co-ordinates on that page, i.e. page 07, co-ordinates 2 3, in Figure 2, were then entered in the space for AAA in Figure 1.

Some pages would then appear diagonally adjacent on a sheet, while others would be vertically or horizontally adjacent, as in Figure 1a.

The printed text of 11 or 12 pages was so arranged that 2 pages were printed on one side of a sheet of paper. Thus 2 pages were permanently associated.

After some time these sheets, each of 2 pages, could be unbound and shuffled so that a completely new arrangement of books resulted. Re-shufflings of this type took place at the beginning of October 1944 and in the middle of February 1945

B.2 Manner of Selection

Formations working with TR.43, especially from the Division forward, were allotted a page by the Chief Signals Officer; selection was made according to the individual's fancy but often the page was used line by line. Such stereotyped usage led to the recognition of callsigns.

The/

* Footnote: A detailed breakdown of approximately 15,000 callsigns was

I 14 f

The High Command networks of the N.K.W.D., often even including the networks of the Regiments forward to Battalions, entered the callsigns selected from TFR.43 (either consecutively or at random) in 10 x 10 squares (100 callsigns). By means of daily changing digit co-ordinates for the squares, it was possible to issue a maximum of 100 callsigns to a W/T station provided with a 2-digit basic number. This system is valid for 3 months.

For example, considering a W/T station with the basic number 31, the callsign on day 1 (see Figure 3) is ÜÜF. The callsign on days 2 and 96 would be NAÜ and STA respectively.

There were 6 vertical co-ordinate columns (for enciphering the 10's digit of the W/T station number) and 6 horizontal co-ordinate rows (for enciphering the 1's digit of the W/T station number), thus yielding 6 x 6 = 36 possible re-ciphers per month. The columns and rows changed monthly; the contents of the square quarterly.

Networks of the Air Force ground areas (R.A.B.) entered the callsigns selected consecutively from TFR.43 in similar squares and then used these squares line per line for 31 days. For the R.A.B. which worked in this manner the same callsigns and meaning recurred every calendar month.

To W/T stations with callsign books 3-digit W/T station numbers were issued. Up to 1,000 W/T stations could thus undertake daily change of callsign by means of one book. The W/T station number was changed daily, by simple substitution tables, into another 3-digit number which then indicated

1) The page in the book;
2) The 10's digit on that page;
3) The 1's digit on that page; -

therefore the callsign for the day.

Figure 4 shows the arrangement for daily encipherment of the W/T station number, together with one example.

The substitution rows (each of 10 digits), shown in Figure 4, were extracted from a table of 100 rows, numbered 1 - 100, which from June to October 1944 were derived by cyclical substitution from 17 basic rows such as were also used in the 3-figure address code with, of course, quite another daily arrangement.

(Ed. Comment: Heimann could not give further details of the address code.)

Figure 5 gives a sample substitution row table.

The substitution rows to be used on each day were detailed in another table valid for 3 months. (See Figure 6.) Against the date in each month were shown 3 numbers each indicating one of the rows in the substitution row table of Figure 5. Each number occurred once only in each column throughout the 3 months.

The original Russian W/T station basic numbers thus obtained

I 19/

agreed exactly with the numbering sequence of the several callsign pages. Indeed the original basic numbers emerged in such a regular order for the entire Russian Front that the A/T station numbers of the 2nd and 3rd Ukranian Fronts were known a long time before they appeared in A/T traffic. The allotment of numbers to the networks of the various Fronts (who used one book between them) is approximately as shown in Figure 7. Figure 8 is a schematic of the square in Figure 7 wherein the shaded portions were operational allotments and the unshaded portions were for reserve allotments.

Similar arrangements for allotting A/T station numbers obviously existed in connection with each of the other books, any pattern, as in Figure 8, depending upon the individual Chief Signals Officer controlling the use of each book.

B. 3 Groups of Callsign Users

The General Staff networks used their own callsign book up till about February 1945. After this date the book used was not identified in other traffic. Both books seem to have been reserved for the General Staff and/or the "Directions" networks.

The High Command networks (Front Armies, Front Corps) used their own book only from July 1944 to March 1945, so that networks of these calls could be claimed as Front Command networks.

There were 4 books for the networks of Armies, Air Armies and also for Corps networks. The Armies of two or three separated fronts employed one book jointly so that only by D/F. etc. was it possible to establish that an Army belonged to one definite Front.

The groups of users had to be determined anew after every shuffling of the pages of the books. No difficulties emerged. On the contrary, every new shuffling revealed new insights. For example the last one in April 1945. It was established, as had been theoretically deduced earlier, that the books of the Command networks contained an additional 11th page, which was not affected by the enciphering process and served to select emergency callsigns, which then were used as permanent callsigns. The books of the Army networks even had two additional pages.

------oOo------

I 19f

P.W. Interrogator's Note:

The members of KONA 1's T.A. party were, by comparison with, say LOEFFLER, very woolly-headed. During interrogation (two at a time) they drifted backwards and forwards persuading one another with disconcerting ease of another version of their story.

This is perhaps not so serious now; it is clear from their account during interrogation that the callsign systems they describe are no longer valid.

------oOo------

I 19 f

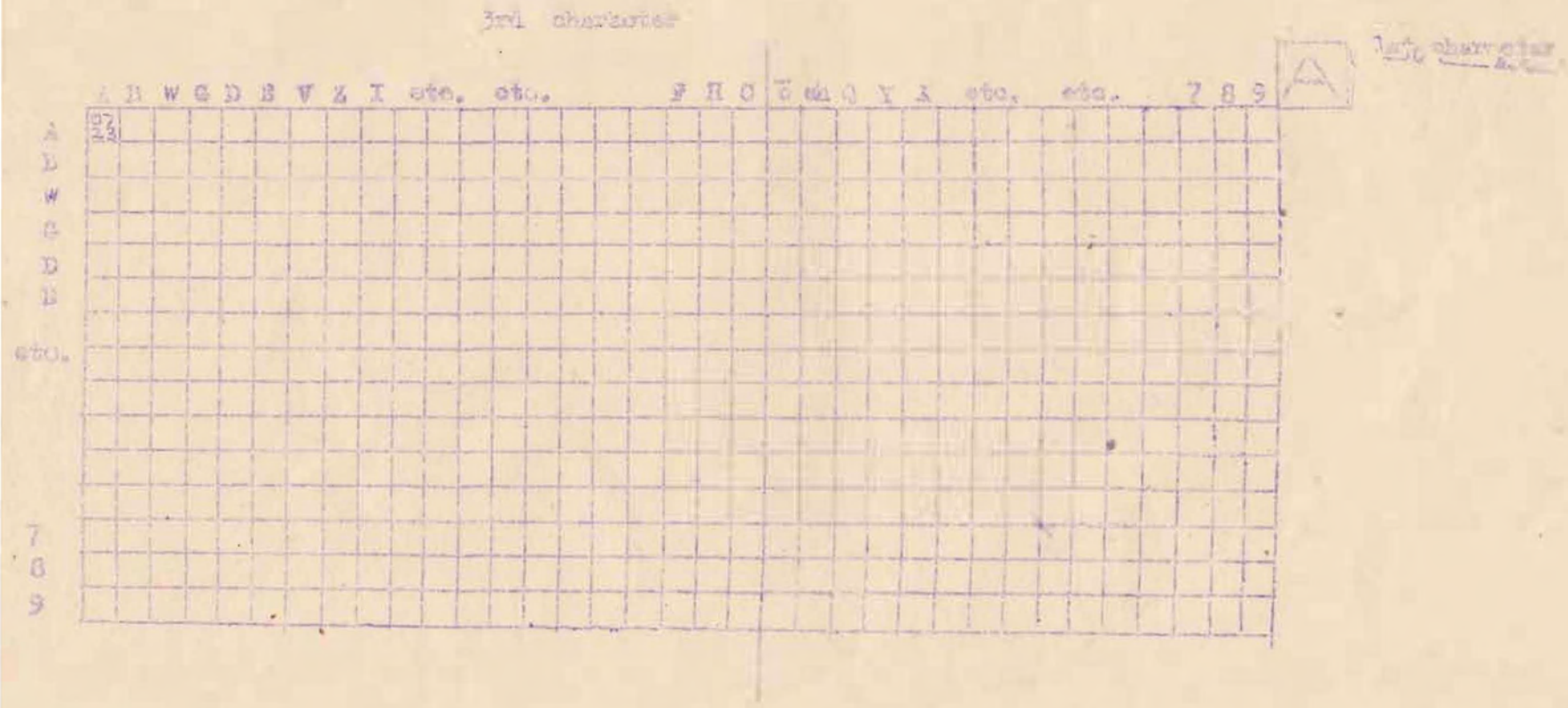
Editor's Summary

The Callsign Book system detailed above is a continuation from a previously known system. The production of Books was by the same method but the manner of callsign selection by encipherment of A/T station basic numbers is new. The latter is almost identical to that used by the Germans after November 1944, and probably influenced the German method. On the other hand, whilst the Germans encoded a callsign determined by the enciphered basic number, the Russians merely used the enciphered number for determining directly page, line and column in the Callsign Book.

Consequently the German system is unbreakable without, say, captured data; the Russian is quite breakable given sufficient callsigns and day-to-day continuity.

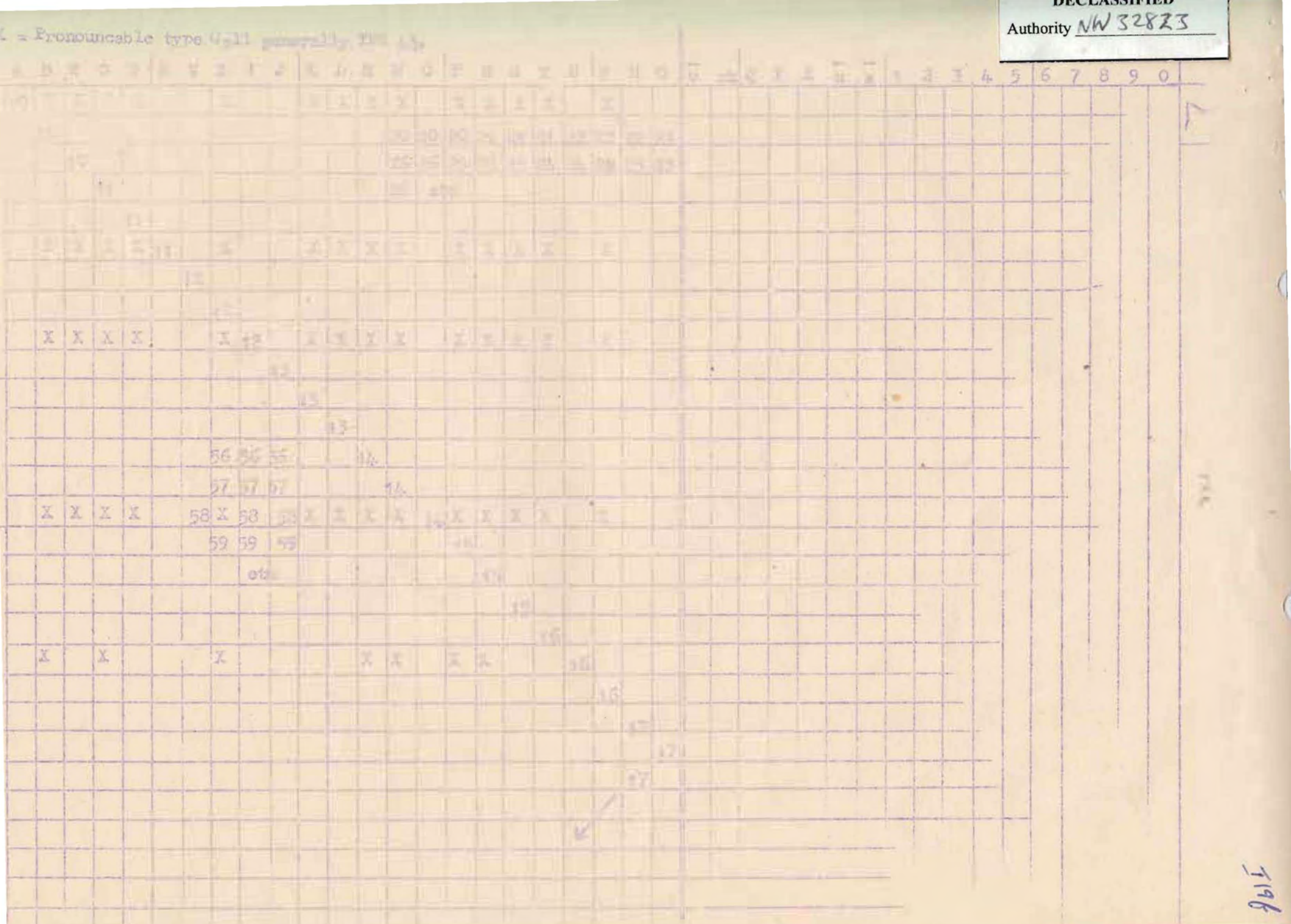
If the system no longer exists it may be that capture of the German system may have in turn influenced the Russians to apply a new and unbreakable process to the encipherment of basic A/T number.

Very little information could be obtained from others to augment Heimann's useful contribution. T.A. was done entirely on traffic continuity (pad numbers, originator's serial numbers, etc.) callsign knowledge, some co-ordination of map co-ordinates, any available decoded material and D/F.



T19f

= Pronouncable type words generally



1's Digit

07

10's Digit	0	1	2	3	4	5	6	7	8	9
0	7BT									
1										
2				[illegible]						
3	FUR	VTX								
4										
5										
6										
7										
8										
9										

Fig. 5

Page in Callsign Book

6 Horizontal Co-ordinate Rows

Day (or Date)

6 Vertical Co-ordinate Columns

2		96	3	1	9	8	5		
	1		8	9	1	0	7		
			7	3	5	1	9		
9	5	6	BAC	BAL	DUM	SCM			
0	3	1	FAM	ARC	CUP	LSN			
4	7	3	MOJ	STA	HOG	EOL			
5	6	9	WGL	SIT					
3	2	0		NAS					
		8							

100 Callsigns

I19f

Date 7.5.45

Digits in A/T Number	0	1	2	3	4	5	6	7	8	9
100's digit substitution (1)	5	7	2	6	0	8	1	3	9	4
10's " " (2)	6	4	5	2	7	3	0	8	9	7
1's " " (3)	2	8	4	6	0	7	5	3	1	9

Substitution "Rows"

Fig. 4

Example; A/T Basic Nr. = 587
Enciphered Nr. = 893
giving Page 8, vertical co-ordinate 9,
horizontal co-ordinate 3

SUBSTITUTION NO. TABLE

1	5	7	2	6	0	8	1	3	9	4
2	9	5	1	3	2	4	6	8	7	0
3										
4				etc.						
etc.				"	"					
"				"	"					
"				"	"					
"				"	"					
100				"	"					

Fig. 5

[illegible]

Date	(1)	(2)	(3)	Date	(1)	(2)	(3)	Date	(1)	(2)	(3)
1	[illegible]	[illegible]	[illegible]	1	[illegible]	[illegible]	[illegible]	1	97	[illegible]	[illegible]
2	[illegible]	[illegible]	[illegible]	2	[illegible]	[illegible]	[illegible]	2	[illegible]	[illegible]	[illegible]
3				3				3			
etc.				etc.				etc.			
31	[illegible]	42	25	31	[illegible]	10	[illegible]	31	[illegible]	[illegible]	[illegible]

Fig. 6

ALLOTMENT OF BASIC NUMBERS TO FRONTS

10's Digit of W/T Stn. Nr.

100's Digit of W/T Stn. Nr.

	0	1	2	3	4	5	6	7	8	9
0	KAF									
1										
2								[illegible]	[illegible]	
3							1W	20	20	
4						1W	10	20		
5					2W	3U	20			
6										
7										
8										
9										

Fig. 7

SCHEMATIC OF FIG. 7

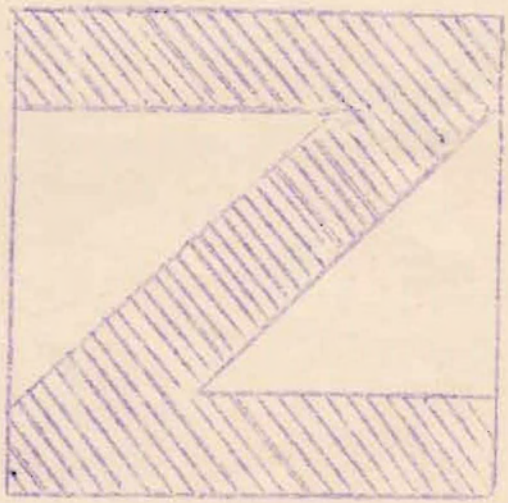


Fig. 8